

ABSTRACT OF THE DISCLOSURE

There are disclosed an extended key generator,  
encryption/decryption unit, and storage medium, in  
which as each of key transform functions, a transform  
5 process is done by an S box (substitution table) on the  
basis of a first key obtained from the inputted key,  
and an adder computes a corresponding one of extended  
keys on the basis of a value obtained by shifting the  
transformed result of the S box to the left, and a  
10 second key obtained from the inputted key.